DENTONS

Liability for cybercrime: a flexible balancing test

Grow | **Protect** | Operate | Finance

September 2024

Detection and prevention of cyberattacks is a constant challenge because of the fast-paced advancement in technology used by cybercriminals. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money through ransomware or interrupting business processes to achieve other ulterior motives.

Taking the right approach to cybersecurity compliance and dealing with incidents swiftly is essential but can be challenging. Ugandan law and practice, like that of other jurisdictions, is often playing "catch up" to the rapid advancement of technology.

To put the threat in perspective, the Uganda Police Force reported in its 2023 Annual Crime Report that cybercrimes led to the loss of over UGX. 1.5 billion (approximately US$400,000) in 2023. This figure does not take into consideration unreported incidents of cybercrime, or the value of data stolen by cybercriminals.

Financial institutions and other businesses need to tighten internal systems and procedures, invest in employee training and raise awareness among clients and the public in order to protect against this growing threat which is bad for business and market growth.

Who is liable for customer losses arising from cybercrime?

Very few cases concerning cyber intrusions make it to court, either because amounts involved are relatively small or because businesses opt for out of court settlements to avoid additional costs and the reputational harm that public court proceedings may bring.

When courts do consider such claims, they look to assign responsibility for the lapse in security to either the business or the customer. The key question is who is best placed to prevent the cyberbreach, a criminal act of a third party, the business or the customer? Broadly speaking, businesses are responsible for putting into place appropriate procedures and policies to prevent a cyberbreach, while customers are also expected to protect themselves.

Cybersecurity litigation in Uganda is dominated by cases involving banks. In the absence of legislation addressing electronic banking, the liability for losses arising from cybercrimes is determined based on the law of negligence and the contract between the bank and its customer.

Under Ugandan law, to prove liability for negligence, the bank must owe the customer a duty of care, which the bank must breach in a manner which caused the specific harm to the customer. The question of whether a duty of care is breached is determined by whether the bank acts in a manner that a reasonable person in their position would. A bank is not legally obliged to take all possible steps to avoid harm; rather the precautions taken by a bank must be practical, taking into account the likelihood of harm and the risks and costs involved.

The High Court of Uganda has issued a number of rulings that define the responsibilities of banks and their customers, based on the law of negligence.

In its latest decision delivered in 2024 in *Stanbic Bank Uganda Limited v Gabigogo (Civil Appeal 28 of 2023)*, the High Court of Uganda ruled that *"banks will only be liable for a breach of the imposed duty which occurs when the burden and utility weigh less than the gravity and likelihood of the harm."* In this case, criminals tricked the respondent and swapped his ATM card while he attempted to deposit money at the ATM. The criminals also read his PIN over his shoulders and thereafter withdrew money from his account. The respondent sued the bank, alleging that it breached its duty of care by failing to provide security guards at the ATM. The Court found the appellant bank to have been negligent and to have breached its banker-customer relationship. The decision was appealed.

The Court of Appeal held that the absence of a security guard at the ATM did not cause the customer's loss at the hand of the fraudsters. Striking a balance between the bank and customer responsibilities, the Court held that the customer himself was negligent in failing to take proper care as he typed his PIN at the ATM, especially when approached by a stranger.

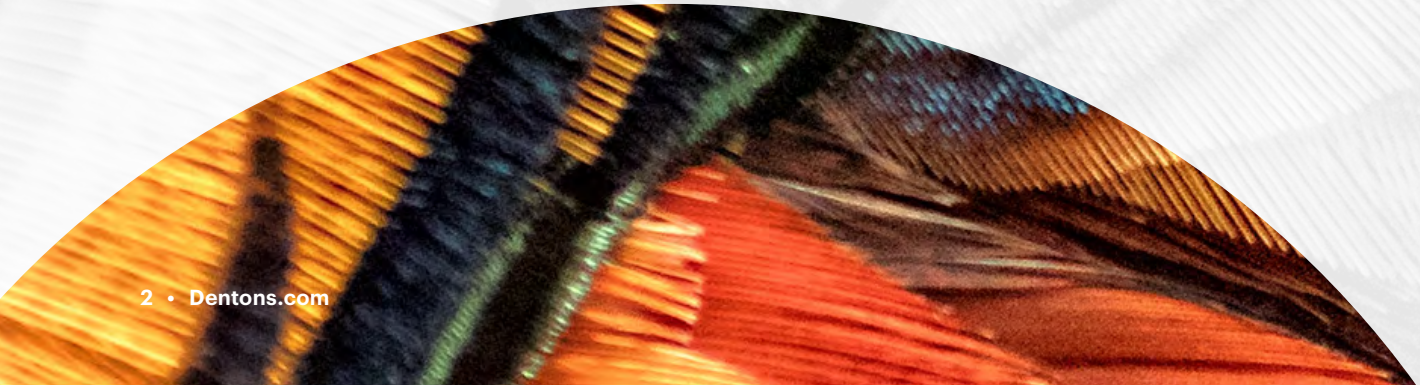
This decision, which is in line with other recent decisions of the High Court, reiterates the general obligation on banks to put in place systems that provide reasonable security to counter the risk of intrusion, taking into account the risk that the bank's security measures are designed to counter.

What security procedures should banks and other businesses have in place to protect against liability for cyberbreaches?

In the *Stanbic Bank Uganda Limited v Gabigogo* case, the Hon. Justice Stephen Mubiru summed up the position at common law: *"A bank will not be held liable once it shows that the security procedure it has in place is a commercially reasonable method of providing security against unauthorised digital payment orders."* As a practical matter this means that internal systems and procedures need to be regularly reviewed and updated.

Banks also owe a general duty of care (in tort) to take reasonable care in relation to the services they provide, and liability for losses will depend on the foreseeability of the risk involved, as well as whether the loss was caused by the specific risk. There is no exact science regarding what protective measures taken by banks will be considered "reasonable" by the Courts and what risks will be considered "foreseeable." However, because cyberfraud is constantly evolving in Uganda and across the world, the duty of care and the foreseeability standard will also change. For example, once banks know that their customers are falling victim to a certain cyberbreach, customers may argue that the risk has become reasonably foreseeable such that the bank has a duty of care to protect against the cyberbreach. This is why most banks now have two factor authentication and SMS notifications for withdrawals, and customer awareness campaigns.

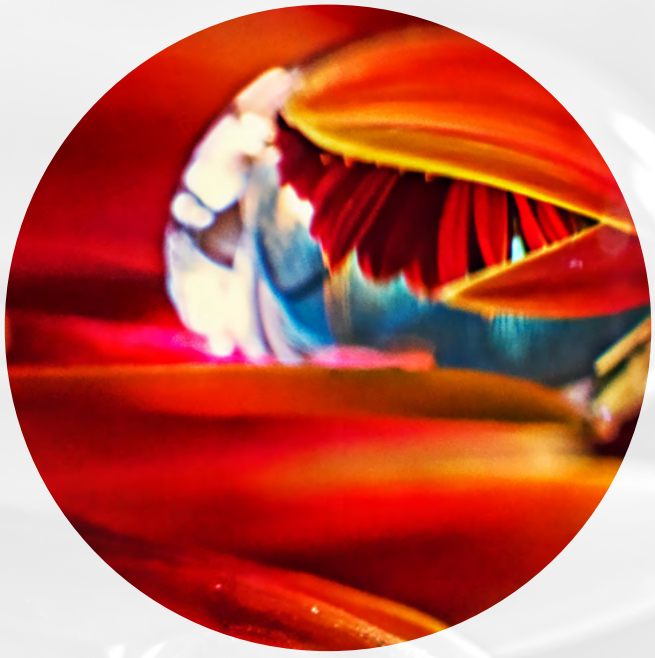
The above decision is consistent with previous decisions such as in *Atiku v Centenary Rural Development Bank Limited (Civil Suit 754 of 2020)* where the High Court ruled that a bank that had proper safeguards, such as two factor authentication and SMS notifications of withdrawals, was not liable for unauthorised withdrawals from its customer's account, considering that the customer had compromised her own security by allowing her daughter to access her mobile phone and know her log in credentials.



How can businesses limit exposure and protect their customers?

In future cases, customers may seek to rely upon the judge's guidance to banks to put in place measures "for ensuring safety and security of electronic banking transactions." To protect and mitigate exposure to future customer claims, banks and businesses should consider adopting these guidelines, which may be viewed as best practice for reasonable protective measures against cybercrime:

- systems which analyse and monitor transactions to identify suspicious transactions;
- regularly checking the authenticity of the customer;
- SMS alerts to customers upon each transaction;
- regular risk assessments;
- awareness programmes on safe cyber transactions for customers and staff;
- repeatedly advising customers about the risks and responsibilities in cyber transactions.



While the above decisions relate to banks, we expect that these same principles will be applied to other businesses at risk where there is a similar duty of care relationship. For example, many jurisdictions are also seeing an increase in online shopping fraud, with more transactions moving online given the increase in smart phone usage and the wide variety of mobile applications.

To avoid reputational harm and potential exposure to liability, banks and other businesses are advised to:

- review contracts with end customers and with the providers of electronic payment or data systems to confirm responsibilities and liability;
- training staff to detect, thwart and manage instances of attempted or actual cyber intrusion;
- two factor authentication for access to accounts and completion of transactions;
- require customers to set strong passwords and to regularly change passwords;
- freeze affected accounts and notify the customer immediately upon occurrence of any suspicious activity.

In case of a data breach, it should also be reported to the Personal Data Protection Office (PDPO) at the National Information Technology Authority – Uganda upon discovering the breach. Although the period is not defined by law, we recommend reporting immediately upon discovering the breach. Uganda's data protection laws do not require the reporting of data breaches to the individuals (Data Subjects) whose data has been compromised. Rather, the PDPO is given the discretion to advise on whether the affected Data Subject should be notified.

Emerging trends in cyber security

Organisations must stay abreast of emerging trends in cyber security so that they can apply and invest in new strategies and developments for preventing and mitigating cyberattacks which expose the financial and corporate sector to reputational harm and potential financial liability. A more detailed guide to dealing with data breaches is available at Dentons - Cybersecurity and Data Breach Response and Dentons - Data Breach Management Tool.

In Singapore, the Cyber Security Agency, which was formed in 2015 with a mandate to protect Singapore's cyberspace, published a recommended standard in January 2024 aimed at enhancing mobile app security and protect against common malware and phishing attempts.

For more information about the best practices set out in Singapore's Cyber Security Agency and the recommended standard, click here: Dentons Rodyk - A guide on the new safety standards to secure high-risk transactions made via mobile applications

In Argentina, the Secretariat of Commerce established that shops that accept credit, purchase or debit cards and operate with electronic terminals will have to make the payment terminals -POS- available to the consumer. The measure keeps the control of the cards in the hands of consumers until the transaction is completed, and therefore prevent fraud by capturing credit, purchase, or debit card data. These measures are being enforced under Argentina's Consumer Defense Law.

For more information about Argentina's measures relating to POS machines, click here: Dentons - Consumers will not have to hand over credit, debit, or prepaid cards in shops

Authors

William Wepukhulu
Associate
D +256 206 300958
william.wepukhulu@dentons.com

Ivan Mushemeza
Associate
D +256 206 300958
ivan.mushemeza@dentons.com